IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF INDIANA
AT EVANSVILLE

MARISSA DUFFY, individually, and on behalf of all others similarly situated, **Plaintiff,** **v.** **LEWIS BROTHERS BAKERIES, INC.** **Defendant.**	Case No. _____

CLASS ACTION COMPLAINT AND JURY DEMAND

Plaintiff, Marissa Duffy, individually, and on behalf of all others similarly situated (hereinafter, "Plaintiff"), brings this Class Action Complaint, against Defendant Lewis Brothers Bakeries Inc. ("Lewis Brothers" or "Defendant"), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, members, and/or other related entities, and upon personal knowledge as to her own actions, and information and belief as to all other matters, alleges as follows:

INTRODUCTION

1. This action arises out of the public exposure of the confidential, private information of Lewis Brothers's current and former employees, as well as potentially its customers (the "Data Breach").

2. According to the data breach notification letter that Defendant sent to Plaintiff, the Data Breach included at least her full name and social security number.

3. As a condition of employment, Defendant required its employees to provide it with their sensitive Private information, which implicitly promised to reasonably safeguard in

compliance with industry standards.

4. Rather than live up to these basic industry standard cybersecurity measures, Defendant skirted its duties and failed to serious invest in the necessary protections to guard against the theft of the critical personal information of its employees and potentially its customers, which then allowed cybercriminals to gain access to the same.

5. Indeed, "[t]here is a common-sense expectation . . . that social security numbers are best kept private and that their exposure to hackers is a harm (whether or not identity theft has yet occurred)."[1]

6. As a direct and proximate result of Defendant's failures to reasonably protect current and former employees' sensitive Private information, Plaintiff and the proposed Class Members have suffered widespread injury and damages and must now deal with the challenge of having their social security number (which they cannot reasonably change) in the hands of cybercriminals who steal identities and extort victims for a living.

PARTIES

7. Plaintiff is a natural person and resident and citizen of the State of Missouri, where she intends to remain.

8. Plaintiff resides in Sullivan, Missouri, and is a former employee of Defendant.

9. Defendant is a corporation organized and existing under the laws of the State of Missouri with its principal place of business at 1220 West Michigan Street, Evansville, Indiana 47710.

10. Defendant's Registered Agent for Service of Process is CT Corporation System, 334 North Senate Avenue, Indianapolis, Indiana 46204.

[1] *Krupa v. TIC Int'l Corp.*, No. 1:22-cv-01951, 2023 WL 143140, at *2 (S.D. Ind. Jan. 10, 2023).

JURISDICTION & VENUE

11. Jurisdiction is proper in this Court under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one class member is a citizen of a state different from Defendant.

12. This Court has personal jurisdiction over Defendant because its principal place of business is located in this State and this District, where Defendant routinely conducts its business.

13. Venue is proper under 28 U.S.C. § 1391 because Defendant's principal place of business of business is located in this District.

COMMON FACTUAL ALLEGATIONS

14. Defendant is a large bakery company, employing around 2000 people and provides bakery products in seventeen states.[2]

15. On or about May 9, 2024, Defendant began sending notification letters to affected persons, informing them that it allowed their personal information to fall into the hands of a cybercriminal gang.

16. According to the notification letter that Defendant sent to Plaintiff, that disclosure *included* Plaintiff's name and social security number.

17. On April 1, 2024, Defendant discovered that a threat actor, now believed to be Medusa, had deployed ransomware on their information systems after having infiltrated Defendant's information systems a week prior.

18. The Medusa ransomware threat is not new and has been the subject of several warnings and publications, some of which have warned that threat actors associated with the

[2] https://lewisbakeries.net/about (last visited May 16, 2024).

Medusa ransomware often engage in multi-extortion tactics whereby they both exfiltrate data and encrypt the target's systems.[3]

19. Defendant's vague letter fails to illuminate how the threat actors gained entry into Defendant's systems or what safeguards Defendant intends to implement to prevent such a breach in the future.

20. Nevertheless, Defendant encourages Plaintiff and the Class to remain vigilant against future threats because of the disclosure of their social security number, including by "reviewing your account statements and monitoring your free credit reports for suspicious activity." Exhibit A.

21. Plaintiff expected that Defendant would adhere to its duty to protect her private information. Indeed, Defendant purports to "respect our workers and their safety."[4]

22. Though Defendant purports to take Plaintiff's privacy seriously, they offered a mere one year of credit monitoring services, which is woefully inadequate to protect against the harms Plaintiff now faces as a result of Defendant's failures.

23. Indeed, Defendant's cybersecurity preparedness is so inadequate that it has not even published a privacy or security policy to its public website.[5]

24. Because of Defendant's failure to implement reasonable and industry standard cybersecurity safeguards, the cybercriminals were able to peruse Defendant's network unseen for a week.

25. The threat actors then stole the private data, including social security numbers of at

[3] *#StopRansomware: MedusaLocker,* CISA.gov (June 30, 2022), https://www.cisa.gov/news-events/alerts/2022/06/30/stopransomware-medusalocker; *Medusa Ransomware on the Rise: From Data Leaks to Multi-Extortion*, THE HACKER NEWS (Jan. 12, 2024), https://thehackernews.com/2024/01/medusa-ransomware-on-rise-from-data.html.
[4] https://lewisbakeries.net/wp-content/uploads/2020/09/Lewis-Bakeries-Corporate-Responsibility-2020.pdf.
[5] https://lewisbakeries.net.

least 13,501 victims, all without being seen by Defendant until it was too late.

26. On information and belief, if Defendant had invested in basic, industry standard monitoring and logging systems, it would have caught the intruders in time to prevent the disclosure of Plaintiff's and Class's private data, including their social security numbers.

27. Shortly after the Data Breach, Medusa posted information regarding the leak on the dark web and demanded a $1,000,000 ransom from Defendant in exchange for the approximately 116 GB of data they were able to exfiltrate under Defendant's nose.[6]

28. Given the amount of data stolen, Plaintiff reasonably believes that Defendant has underrepresented the categories of personal information affected.[7]

A. Plaintiff's Experience.

29. Plaintiff is a former employee of Defendant and received a notification letter informing her that Defendant's Data Breach included her social security number. Exhibit A.

30. As a condition of employment, Defendant required that Plaintiff divulge her social security number to it.

31. Plaintiff is exceedingly careful with her personal information because she is aware of the ubiquitous nature of cyber malicious activity.

32. In entrusting her private information to Defendant as a condition of employment, Plaintiff believed that Defendant would adequately safeguard that information. Had Plaintiff known that Defendant did not employ reasonable data security measures, Plaintiff would not have entrusted her private information to Defendant.

33. Based on Defendant's purported investigation, Plaintiff now understands that her

[6] https://www.privacyaffairs.com/medusa-ransomware-actors-hit-multiple-targets.
[7] According to Breach Sense, Defendant's breach included 115.92 GB of data. https://www.breachsense.com/breaches/lewis-brothers-bakeries-data-breach.

social security number is in the hands of cybercriminals whose occupation is identity theft and extortion.

34. Because these criminals now have her social security number, and because Defendant instructed her to remain vigilant and monitor her accounts, credit, and statements, Plaintiff has spent multiple hours attempting to combat the threat she now faces—including by monitoring accounts, pouring over her financial statements to look for fraudulent transactions, and monitoring her credit.

35. As a direct and proximate result of the Data Breach permitted to occur by Defendant, Plaintiff has suffered, and imminently will suffer, injury-in-fact and damages, including the violation of her valuable privacy, a heightened risk of identity theft because her social security number (which she cannot change) is now in the hands of cybercriminals, monetary harms in the forms of her lost time spent at Defendant's direction, and the future monetary harm that she will incur by having to spend even more time performing those same tasks at Defendant's direction of because of Defendant's failures. Moreover, Plaintiff has and will continue to suffer severe mental and emotional distress, fear, worry, and anxiety over the looming threat to her financial well being because of Defendant's egregious failures.

36. Indeed, as a result of Defendant's Data Breach, its victims face a lifetime risk of identity theft, and increased risk of harm because the Data Breach included their social security numbers.

37. Moreover, even if Plaintiff's information has not already been published to even more cybercriminals and the public at large, Plaintiff knows that such a further disclosure is imminent because it is the modus operandi of the Medusa ransomware gang—who is known to perform multi-extortion events and will leak the stolen data publicly if Defendant refused to pay

the ransom.[8]

B. This Data Breach was Foreseeable by Defendant.

38. Defendant tortiously failed to take the necessary precautions required to safeguard and protect the private information of Plaintiff and the Class Members from unauthorized disclosure. Defendant's actions represent a flagrant disregard of Plaintiff's and the other Class Members' rights.

39. Plaintiff and Class Members were the foreseeable and probable victims of Defendant's inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing private information and the critical importance of providing adequate security for that information.

40. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.[9]

41. According to the Identity Theft Resource Center's January 24, 2022 report for 2021, "the overall number of data compromises (1,862) is up more than 68 percent compared to 2020. The new record number of data compromises is 23 percent over the previous all-time high (1,506) set in 2017. The number of data events that involved sensitive information (Ex: Social Security numbers) increased slightly compared to 2020 (83 percent vs. 80 percent)."[10]

42. The increase in such attacks, and the attendant risk of future attacks, was widely known to the public and to anyone motivated to look. According to IBM's 2022 report, "[f]or 83%

[8] Miklos Zoltan, *MEDUSA Ransomware Actors Hit Multiple Targets*, PRIVACY AFFAIRS (May 1, 2024), https://www.privacyaffairs.com/medusa-ransomware-actors-hit-multiple-targets ("The operators also employ a multi-extortion tactic, encrypting the victim's files and stealing data for ransom. If the victim refuses to pay, MEDUSA will leak the data publicly. This can impact the victim's reputation considerably.").
[9] https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last accessed Dec. 7, 2022).
[10] *See* "Identity Theft Resource Center's 2021 Annual Data Breach Report Sets New Record for Number of Compromises," Jan. 24, 2022, available at https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/ (last acc. Apr. 14, 2023).

of companies, it's not if a data breach will happen, but when."[11]

43. Private information is of great value to hackers and cybercriminals, and the data compromised in the Data Breach can be used for a variety of unlawful and nefarious purposes, including ransomware and fraudulent misuse, and sale on the Dark Web, especially consider Medusa's tendency to publish such data on the Dark Web.

44. Private information can be used to distinguish, identify, or trace an individual's identity, such as their names, social security numbers, and medical records. This can be accomplished alone, or in combination with other personal or identifying information that is connected, or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.

45. Given the nature of the Data Breach, it was foreseeable that the compromised Private information could be used by cybercriminals in a variety of different injurious ways. Indeed, the cybercriminals who possess the Plaintiff's and Class Members' Private information can easily obtain their tax returns or open fraudulent credit card accounts in their names.

46. As the Social Security Administration has recognized, a cybercriminal that gains access to a victim's social security number can use that information to gain access to get more information about the victim or to steal the victim's identity:

> Every year, millions of Americans become victims of identity theft. Identity theft occurs when someone steals your personally identifiable information and pretends to be you. They can use this information to open bank or credit card accounts, file taxes, or make new purchases in your name.
>
> It is important that you take steps to protect your Social Security number from theft. If someone obtains your Social Security number, they can use it to get other personal information about you, including your bank or credit information.[12]

[11] IBM, "Cost of a data breach 2022: A million-dollar race to detect and respond," available at https://www.ibm.com/reports/data-breach (last acc. Apr. 14, 2023).

[12] Doug Walker, *Protection Your Social Security Number From Identity Theft*, SOCIAL SECURITY MATTERS (last updated: Nov. 3, 2023), https://blog.ssa.gov/protecting-your-social-security-number-from-identity-theft.

C. Defendant Fails to Comply with Industry Standards.

47. Cybersecurity experts routinely identify organizations holding personally identifiable information as being particularly vulnerable to cyberattacks because of the value of the information they collect and maintain.

48. Many industry and national best practices have been published and are widely used as a go-to resource when developing an institution's cybersecurity standards. The Center for Internet Security's (CIS) CIS Critical Security Controls (CSC) recommends certain best practices to adequately secure data and prevent cybersecurity attacks, including 18 Critical Security Controls of Inventory and Control of Enterprise Assets, Inventory and Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses, Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security Awareness and Skills Training, Service Provider Management, Application Software Security, Incident Response Management, and Penetration Testing.[13]

49. In addition, the National Institute of Standards and Technology (NIST) recommends certain practices to safeguard systems, *infra,* such as:

a. Controlling who logs on to your network and uses your computers and other devices;

b. Using security software to protect data;

c. Encrypting sensitive data, at rest and in transit;

d. Conducting regular backups of data;

[13] *See* https://www.rapid7.com/solutions/compliance/critical-controls/ (last acc. Apr. 14, 2023).

e. Updating security software regularly, automating those updates if possible;

f. Having formal policies for safely disposing of electronic files and old devices;

g. Training everyone who uses your computers, devices, and network about cybersecurity.[14]

50. Upon information and belief, Defendant failed to meet the minimum standards of both the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established frameworks for reasonable cybersecurity readiness, and other industry standards for protecting Plaintiff's and the proposed Class Members' Private information, resulting in the Data Breach.

51. Moreover, multi-factor authentication is unquestionably industry standard. "Nowadays, multi-factor authentication (MFA) is the industry standard for identity and access verification purposes."[15]

D. Defendant Failed to Comply with FTC Guidelines

52. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

53. In 2016, the FTC updated its publication, *Protecting Private information: A Guide*

[14] Understanding The NIST Cybersecurity Framework, https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework (last acc. Apr. 14, 2023).
[15] James Stanger, *Multi-Factor Authentication: A Primer for Today's IT Professional*, COMPTIA (Sept. 25, 2023), https://www.comptia.org/blog/multi-factor-authentication.

for Business, which establishes cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of Private information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[16]

54. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[17]

55. The FTC has brought enforcement actions against businesses for failing to reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

56. These FTC enforcement actions include actions against entities failing to safeguard PII such as Defendant. *E.g.*, *In the Matter of LabMD, Inc., A Corp*, 2016-2 Trade Cas. (CCH)

[16] *See* Federal Trade Commission, October 2016, "Protecting Private information: A Guide for Business," available at https://www.bulkorder.ftc.gov/system/files/publications/2_9-00006_716a_protectingpersinfo-508.pdf (last acc. Apr. 14, 2023).
[17] *See id*.

¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

57. Defendant failed to properly implement basic data security practices widely known throughout the industry. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patient Private information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

58. Defendant was at all times fully aware of its obligations to protect the Private information of Defendant's patients that was entrusted to Defendant. Defendant was also aware of the significant repercussions that would result from their failure to do so.

59. Because of Defendant's failure to adhere to these basic cybersecurity industry standards, which resulted in the disclosure of the necessary ingredients to conduct identity theft and fraud, Plaintiff and the Class now must face the threat of identity theft and fraud for the rest of their lives.

E. The Data Breach Caused Plaintiff and the Class Members Injury and Damages

60. Plaintiff and the putative Class have suffered injuries and damages from the unauthorized disclosure and misuse of their private information that can be directly traced to Defendant, that has occurred, is ongoing, and will imminently occur.

61. The ramifications of Defendant's failure to keep Plaintiff's and the Class's private information secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, social security number, driver's license number, date of birth, or other information, such as addresses, without permission, to commit fraud or other crimes. Importantly, simply gaining access to an individual's social security

number puts those individuals are immense risk of identity theft and that risk continues because the victim cannot reasonably change their social security number.

62. Because Defendant failed to prevent the Data Breach, Plaintiff and the proposed Class Members have suffered, will imminently suffer, and will continue to suffer injury-in-fact and damages, including monetary losses, lost time, anxiety, and emotional distress. Plaintiff and the Class Members have suffered, and will imminently suffer:

a. The loss of the opportunity to control how private information is used, which is a core privacy principle;

b. Unauthorized use of stolen private information, which is now in the hands of cybercriminals and is at imminent threat of publication to even more criminals and the public at large because of Medusa's threat to publish if the ransom is not paid;

c. Emotional distress;

d. Out-of-pocket expenses associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost time that Plaintiff and the Class spent at Defendant's direction to attempt to ward off the perils associated with Defendant's failure to reasonably safeguard sensitive data it collected, including time spent researching how to prevent, detect, contest, and recover from identity theft and fraud, monitoring accounts and financial statements, and monitoring and freezing credit;

f. Delay in receipt of tax refund monies; and,

g. The continued risk to their private information, which remains in the

possession of Defendant, and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the private information in its possession.

63. Furthermore, the Data Breach has placed Plaintiff and the proposed Class Members at an increased risk of fraud and identity theft because the Breach included their social security numbers.

64. The myriad dangers associated with Defendant's Data Breach, include cybercriminals opening new financial accounts, credit cards, and loans in victim's names; hackers taking over email and other accounts; time and effort to repair credit scores; losing home due to mortgage and deed fraud; theft of tax refunds; delays in receiving tax refunds; hackers posting embarrassing posts on victim's social media accounts; victims spending large amounts of time and money to recover their identities; experiencing psychological harm and emotional distress; victims becoming further victimized by repeat instances of identity theft and fraud; cybercriminals committing crimes in victim's names; victims' personal data circulating the Dark Web forever; victims receiving increased spam telephone calls and emails; victims' children or elderly parents having their identities stolen.[18]

65. Indeed, because Defendant allowed Plaintiff's and the Class's social security numbers to be leaked, the Medusa gang is now likely about to access the full gambit of Plaintiff's privacy and sensitive information, and nonetheless is freely able to conduct the full range of financial fraud and identity theft.

66. The FTC recommends that identity theft victims take several costly steps to protect

[18] *See* Gaetano DiNardi, Aura.com, "How Bad Is Identity Theft? Is It Serious?" (December 14, 2022) available at https://www.aura.com/learn/dangers-of-identity-theft#:~:text=Fraudsters%20can%20open%20new%20accounts,to%20repair%20your%20credit%20score (last acc. Feb. 27, 2023).

their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity, not just a single year), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, seeking a credit freeze, and correcting their credit reports.[19]

67. Identity thieves use stolen Private information such as social security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

68. Identity thieves can also use social security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and social security number to obtain government benefits; or file a fraudulent tax return using the victim's information.

69. In addition, identity thieves may obtain a job using the victim's social security number, rent a house or receive medical services in the victim's name, and may even give the victim's private information to police during an arrest—resulting in an arrest warrant being issued in the victim's name. That can be even more problematic and difficult to remedy for someone who already has a criminal record.

70. Further, according to the Identity Theft Resource Center's 2021 Consumer Aftermath Report, identity theft victims suffer "staggering" emotional tolls: "For example, nearly 30% of victims have been the victim of a previous identity crime; an all-time high number of victims say they have contemplated suicide. Thirty-three percent reported not having enough money to pay for food and utilities, while 14% were evicted because they couldn't pay rent or their

[19] *See* https://www.identitytheft.gov/Steps (last visited September 1, 2021).

mortgage. Fifty-four percent reported feelings of being violated." [20]

71. The value of sensitive information is axiomatic; one need only consider the value of Big Data in corporate America, or that the consequences of cyber theft include heavy prison sentences. Even the obvious risk to reward analysis of cybercrime illustrates beyond doubt that Private information has considerable market value.

72. Moreover, there is often a substantial time lag–measured in years–between when harm occurs versus when it is discovered, and also between when private information and/or financial information is stolen and when it is used.

73. Social Security numbers are among the worst kind of Private information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud.[21]

74. For example, the Social Security Administration has warned that identity thieves can use an individual's social security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[22] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her social security Number was used to file for unemployment benefits until law enforcement notifies the individual's

[20] *See* Jason Steele, *Credit Card and ID Theft Statistics*, CreditCards.com (June 11, 2021), avail. at https://www.creditcards.com/statistics/credit-card-security-id-theft-fraud-statistics-1276/ citing Identity Theft Resource Center, 2021 Consumer Aftermath Report (May 26, 2021), https://www.idtheftcenter.org/post/the-identity-theft-resource-centers-2021-consumer-aftermath-report-reveals-impacts-on-covid-19-identity-crime-victims/ (last acc. Feb. 27, 2023).
[21] *See* U.S. Social Security Administration, "Identity Theft and Your Social Security Number," Publication No. 05-10064, July 2021, available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last acc. Feb. 25, 2023).
[22] *See id.*

employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

75. Moreover, it is not an easy task to change or cancel a stolen social security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[23]

76. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[24]

77. Accordingly, the Data Breach has caused Plaintiff and the proposed Class Members a greatly increased risk of identity theft and fraud, in addition to the other injuries and damages set forth herein, specifically the imminent identity fraud and criminal fraudulent activity, fraudulent charges, theft of monies, and attendant costs; lost time and efforts in remediating the impact of the Data Breach, and other injury and damages as set forth in the preceding paragraphs.

78. Defendant knew or should have known of these harms which would be caused by the Data Breach it permitted to occur and strengthened its data systems accordingly.

CLASS ACTION ALLEGATIONS

116. Plaintiff sues on behalf of herself and the proposed Class, defined as follows:

All United States citizens whose private information was disclosed, accessed,

[23] *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR, Brian Naylor, Feb. 9, 2015, http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited September 1, 2021).

[24] *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, Tim Greene, Feb. 6, 2015, http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited September 1, 2021).

or compromised in the Data Breach experienced by Defendant beginning on or about March 25, 2024.

117. The following people are excluded from the Class: (1) any judge or magistrate presiding over this action and members of their families; (2) Defendant, Defendant's members, partners, subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which Defendant or its parents has a controlling interest, and their current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

118. The Class defined above is identifiable through Defendant's business records.

119. Plaintiff reserves the right to amend the class definition.

120. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

a. Numerosity. Plaintiff is representative of the proposed Class, consisting of potentially thousands but at least 13,501 individuals, which are identifiable based on Defendant's records, and far too many to join in a single action;

b. Typicality. Plaintiff's claims are typical of Class Member's claims as each arises from the same Data Breach, the same alleged violations by Defendant, and were all affected by Defendant's failure to implement reasonable cybersecurity safeguards.

c. Adequacy. Plaintiff will fairly and adequately protect the proposed Class's interests. Plaintiff's interests do not conflict with Class Members' interests and Plaintiff has retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel. Defendant has no defenses unique to

Plaintiff.

d. Commonality. Plaintiff's and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for all Class members. Common questions for the Class include, but are not necessarily limited to the following:

i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's private information;

ii. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

iii. Whether Defendant was negligent in maintaining, protecting, and securing Private information;

iv. Whether Defendant breached contractual promises to safeguard Plaintiff's and the Class's private information;

v. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

vi. Whether Defendant's Data Breach notice was reasonable;

vii. Whether Defendant's conduct was likely to deceive the public;

viii. Whether Defendant is liable for negligence;

ix. Whether Defendant was negligent *per se*;

x. Whether Defendant's practices and representations related to the Data Breach breached implied contracts;

xi. Whether the Data Breach caused Plaintiff and the Class injuries and damages;

xii. What the proper damages measure is; and

xiii. Whether Plaintiff and the Class are entitled to damages, or declaratory and injunctive relief.

121. Further, this action satisfies Fed. R. Civ. P. 23 because: (i) common questions of law and fact predominate over any individualized questions; (ii) prosecuting individual actions would create a risk of inconsistent or varying adjudications, risking incompatible standards of conduct for Defendant, and a risk adjudications with respect to individual Class Members which would as a practical matter be dispositive of the interests of the other members not parties to the adjudications or would substantially impair or impede their ability to protect their interest; and (iii) the Defendant have acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Class as a whole.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

122. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

123. Plaintiff and the Class Members entrusted their private information to Defendant as a condition of employment.

124. Defendant owed to Plaintiff and Class Members a duty to exercise reasonable care the maintenance, handling, and protection of their personal and private information, including to implement industry-standard cybersecurity procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

125. Defendant owed a duty of care to Plaintiff and Class Members because it was

foreseeable that Defendant's failure to reasonably safeguard the private information in accordance with industry standards concerning data security would result in the compromise of that private information—just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and Class Members's private information by disclosing and providing access to this information to third parties and by failing to properly supervise both the way the private information was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

126. Defendant owed to Plaintiff and Class Members a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and Class Members to take appropriate measures to protect their private information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

127. Defendant owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff's and Class Members's private information as a condition of employment.

128. The risk that unauthorized persons would attempt to gain access to the private information, and misuse it, was imminent foreseeable to anyone that bothered to consider the threats faced today by every company that collects and stores such valuable information. Given that Defendant holds vast amounts of private information, it was inevitable that unauthorized individuals would attempt to access Defendant's databases.

129. Private information is highly valuable, and Defendant knew, or should have known,

the risk in obtaining, using, handling, emailing, and storing such private information of Plaintiff and Class Members and the importance of exercising reasonable care in handling it.

130. Defendant breached its duties by failing to exercise reasonable care in supervising its agents and in handling and securing Plaintiff's and Class Members' data, which actually and proximately caused the Data Breach and Plaintiff's and Class Members' injuries.

131. Defendant is further breaching its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and Class Members, in that the approximately 116 GB of data almost certainly contains further unreported information, which can be reasonably inferred based on the amount of data at issue.

132. As a direct, proximate, and traceable result of Defendant's negligence, Plaintiff and the Class Members have suffered or will imminently suffer injury-in-fact and damages, including but not limited to the loss of the opportunity to control how private information is used; unauthorized use of stolen private information; emotional distress; compromise and continuing publication of their private information; out-of-pocket expenses associated with the prevention, detection, recovery, and remediation from identity theft or fraud; lost opportunity costs, lost wages, and/or the lost value of their time given the time and effort expended addressing and trying to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud; delay in receipt of tax refund monies; and, the continued risk to their private information, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the private information in its possession.

133. As a direct and proximate result, Plaintiff and the Class are entitled to recover damages including actual and compensatory damages, nominal damages, and punitive damages,

as permitted by law.

134. Further, Plaintiff and the Class are entitled to injunctive relief ordering Defendant to strengthen its data security systems, monitoring procedures, and data breach notification procedures to prevent additional unauthorized disclosure of the private information in Defendant's possession.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

135. Plaintiff incorporates the above Paragraphs as if fully set forth herein.

146. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' private information.

147. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers or, in this case, patients' Private information. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff's and the Class Members' sensitive Private information.

148. Defendant violated its duties under Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff's and the Class's Private information and by not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of private information Defendant had collected, and stored, and the foreseeable consequences of a Data Breach, including, specifically,

the immense damages that would result to its patients in the event of a breach, which ultimately came to pass.

149. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

150. Defendant had a duty to Plaintiff and the Class Members to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and the Class's Private information.

151. Defendant breached its duties to Plaintiff and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private information, and to supervise their vendors to ensure they did so.

152. Defendant's violations of Section 5 of the FTC Act and their failure to comply with applicable laws and regulations constitutes negligence *per se*.

153. But for Defendant's wrongful and negligent breach of the duties owed to Plaintiff and members of the Class, Plaintiff and Class Members would not have been injured.

154. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that it was failing to meet its duties and that its Data Breach would cause Plaintiff and Class Members to suffer the foreseeable harms associated with the exposure of their private information.

155. Had Plaintiff and Class Members known that Defendant did not adequately protect their Private information, Plaintiff and Class Members would not have entrusted Defendant with their Private information.

156. As a direct, proximate, and traceable result of Defendant's negligence *per se*, Plaintiff and the Class Members have suffered or will imminently suffer injury-in-fact and damages, including but not limited to the loss of the opportunity to control how private information is used; unauthorized use of stolen private information; emotional distress; compromise and continuing publication of their private information; out-of-pocket expenses associated with the prevention, detection, recovery, and remediation from identity theft or fraud; lost opportunity costs, lost wages, and/or the lost value of their time given the time and effort expended addressing and trying to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud; delay in receipt of tax refund monies; and, the continued risk to their private information, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the private information in its possession.

157. As a direct and proximate result, Plaintiff and the Class are entitled to recover damages including actual and compensatory damages, nominal damages, and punitive damages, as permitted by law.

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

159. Plaintiff incorporates the above Paragraphs as if fully set forth herein.

160. Defendant required that Plaintiff provide it with sensitive personal information as

a condition of employment, which Plaintiff and Defendant understood included a concomitant agreement to safeguard that data due to the known harms associated with the exposure of Plaintiff's social security number, among other data.

161. As such, Defendant implicitly agreed it would not disclose the private information it collects to unauthorized persons and that it would reasonably safeguard the same.

162. Plaintiff and the Class Members accepted Defendant's offer by providing Defendant with their social security numbers, among other information.

163. Plaintiff and the Class Members would not have entrusted their private information to Defendant in the absence of such an agreement.

164. Defendant materially breached the contract(s) it had entered into with Plaintiff and the Class Members by failing to reasonably safeguard their private information. Defendant further breached the implied contracts with Plaintiff and the Class Members by:

a. Failing to comply with industry standards, as well as legal obligations that are necessarily incorporated into the parties' agreement; and

b. Failing to properly supervise its agents in possession of private information;

c. Failing to ensure the confidentiality and integrity of electronic private information that Defendant created, received, maintained, and transmitted.

165. The damages sustained by Plaintiff and Class Members as described above were the direct, proximate, and imminently foreseeable result of Defendant's material breaches of its agreement(s).

166. Plaintiff and the Class Members have performed as required under the relevant agreements, or such performance was waived by the conduct of Defendant.

167. The covenant of good faith and fair dealing is an element of every contract. All

such contracts impose upon each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

168. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

169. Defendant's failure to reasonably secure Plaintiff and the Class's data, and its failure to inform them of these critical failures represents a failure to perform the contracts in good faith and the failure to inform Plaintiff and the Class upon hiring them represents a failure to deal in good faith.

170. Defendant's failure to inform Plaintiff and the Class of the full scope of the data now in the hands of cybercriminals is a full such failure.

171. Plaintiff and the Class Members have sustained injuries-in-fact and damages because of Defendant's breaches of its agreement, including breaches thereof through violations of the covenant of good faith and fair dealing.

COUNT IV
INVASION OF PRIVACY—PUBLIC DISCLOSURE OF PRIVATE FACTS
(On Behalf of Plaintiff and the Class)

172. Plaintiff incorporates the above Paragraphs as if fully set forth herein.

173. The Plaintiff and the Class Members took reasonable and appropriate steps to keep their Private information confidential from the public.

174. Plaintiff's and the Class Members' efforts to safeguard their own Private information were successful, as their private information was not known to the general public prior to the Data Breach.

175. Plaintiff and the Class Members had a legitimate expectation of privacy to their private information, entrusted solely to Defendant for purpose of their employment, and were entitled to the protection of this information against disclosure to unauthorized third parties.

176. Defendant owed a duty to its employees, including Plaintiff and the Class Members, to keep their private information confidential.

177. The unauthorized release of private information by Defendant in the Data Breach is highly offensive to a reasonable person, and caused harms long recognized at common law.

178. Plaintiff's and Class Members' information is not of legitimate public concern.

179. Defendant knew or should have known that Plaintiff's and Class Members' private information was private, confidential, and should not be disclosed.

180. Defendant publicized Plaintiff's and Class Members's private information, by unauthorizedly disclosing it to cybercriminals who had no legitimate interest in this Private information and who had the express purpose of monetizing that information through fraudulent misuse and by injecting it into the illicit stream of commerce flowing through the Dark Web.

181. Though Defendant no doubt did not literally intend for cybercriminals to infiltrate its information systems, Defendant knew that such intrusion and theft was reasonably and substantially certain in the absence of industry standard cybersecurity safeguards—as all minimally qualified cybersecurity professionals know.

182. Indeed, not only was Plaintiff's and Class Members's private information exfiltrated from Defendant's systems, but, upon information and belief, has been or will

imminently be published on the Dark Web and used to commit fraud; and is being disseminated amongst, *inter alia,* other criminals, financial institutions, merchants, creditors, health care providers and governmental agencies.

183. It is therefore substantially certain that the Plaintiff's and the Class Members' private information is rapidly becoming public knowledge—among the community at large—due to the nature of the cyber-attack that procured it, and the identity theft for which it is designed.

184. Regardless, Plaintiff's and Class Members's social security numbers are now in the hands of an exceeding large group of cybercriminals operating all over the world.

185. As a direct and proximate result of the public disclosure of private facts committed by Defendant, Plaintiff and the Class Members have suffered injury-in-fact and damages as set forth in the preceding paragraphs.

COUNT V
BAILMENT
(On Behalf of Plaintiff and the Class)

186. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

187. Plaintiff, the Class Members, and Defendant contemplated a mutual benefit bailment when the Plaintiff and putative members of the Class transmitted their Private Information to Defendant solely for the purpose of obtaining employment. Plaintiff and the Class entrusted their Private Information to Defendant for a specific purpose—to obtain employment—with an implied contract that the trust was to be faithfully executed, and the Private Information was to be accounted for when the special purpose was accomplished.

188. Defendant accepted the Plaintiff' sand the Class's Private Information for the specific purpose of employment.

189. Defendant was duty bound under the law to exercise ordinary care and diligence in safeguarding Plaintiff's and the Class's Private Information.

190. Plaintiff's and the Class's Private Information was used for a different purpose than the Plaintiff and the Class intended, for a longer time period and/or in a different manner or place than Plaintiff and the Class intended.

191. As set forth in the preceding paragraphs, Plaintiff and the Class Members were damaged thereby.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, Marissa Duffy, individually, and on behalf of all others similarly situated, requests that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing her counsel to represent the Class;

B. Awarding Plaintiff and the Class damages that include applicable compensatory, actual, exemplary, and punitive damages, as allowed by law;

C. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

D. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

E. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

F. Awarding attorneys' fees and costs, as allowed by law;

G. Awarding prejudgment and post-judgment interest, as provided by law;

H. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

I. Granting such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

Plaintiff demands a trial by jury on all issues so triable.

Dated: May 17, 2024

Respectfully submitted,

/s/ Lynn A. Toops
Lynn A. Toops (No. 26386-49)
Amina A. Thomas (No. 34451-49)
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, Indiana 46204
Telephone: (317) 636-6481
ltoops@cohenandmalad.com
athomas@cohenandmalad.com

J. Gerard Stranch, IV*
Grayson Wells*
STRANCH, JENNINGS & GARVEY, PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200
Nashville, Tennessee 37203
(615) 254-8801
(615) 255-5419 (facsimile)
gstranch@stranchlaw.com
gwells@stranchlaw.com

**Pro Hac Vice* forthcoming

Counsel for Plaintiff and the Proposed Class